REMARKS

This response is intended as a full and complete response to the non-final Office Action mailed August 10, 2005. In the Office Action, the Examiner notes that claims 1-9 are pending of which claims 1-6 are allowed and claims 7-9 are rejected. By this response, claims 7-9 have been amended.

In view of both the amendments presented above and the following discussion, Applicant submits that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. §103. Thus, Applicant believes that all of these claims are now in allowable form.

It is to be understood that the Applicant, by amending the claims, does not acquiesce to the Examiner's characterizations of the art of record or to Applicant's subject matter recited in the pending claims. Further, Applicant is not acquiescing to the Examiner's statements as to the applicability of the art of record to the pending claims by filing the instant response.

Amendments to the claims

By this response, claims 7-9 have been amended. The amendments to the claims are fully supported by the Specification, Drawings and Claims as originally filed. For example, the amendments to claim 7 are supported at least by page 7, lines 12-29. The amendments to claims 8-9 are cosmetic. Thus, no new matter has been added and the Examiner is respectfully requested to enter the amendments to the claims.

Allowable Subject Matter

Applicant respectfully thanks the Examiner for the allowance of claims 1-6.

35 U.S.C. §103 Rejection of Claims 7-9

Claims 7-9 are rejected under 35 U.S. C. §103(a) as being unpatentable over U.S. Patent Application Publication Number 2002/0031134 published March 14, 2002 to Poletto et al. (hereinafter Poletto) in view of Dacier et al., U.S. Patent No. 6,487,204 B1 (hereinafter "Dacier").

Claim 7

To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. The Poletto and Dacier references fail to teach or suggest all of the limitations recited in claim 7, and thus fail to teach or suggest the Applicants' invention as a whole.

Specifically, the Poletto and Dacier references do not teach or suggest at least the "establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet" (emphasis added) as recited in the claim as amended.

Poletto discloses "a system architecture for thwarting denial of service attacks on a victim data center" (abstract). However, as the Examiner acknowledges:

> "... Poletto does not explicitly teach whereby said TCP proxy, when subject to a CSDOS attack, does not successfully establish a TCP connection with said malicious host, and no TCP connection is made from said TCP proxy to said server, thereby protecting said server from said attack." (page 3 of the 8/10/05 Office Action, emphasis added)

The Dacier reference fails to bridge the substantial gap between the Poletto reference and the Applicant's invention. The Dacier reference discloses a switch in an ATM network which operates in a learning mode and an active mode. Regarding the Dacier reference, the Examiner alleges:

> "In the same field of endeavor, Dacier teaches a system and method wherein malicious attacks are detected wherein a connection is not established absent and acknowledgement packet (See Dacier, col. 1, lines 14-52). It would have been obvious to one having ordinary skill in the art at the time the invention was made to have incorporated the acknowledgment of Dacier into the system of Poletto for the purpose of protecting a network from malicious attacks." (page 3 of the 8/10/05 Office Action, emphasis added)

Thus, the Examiner alleges that the Dacier reference teaches a connection is not established absent an acknowledgement packet. However, the Applicants respectfully disagree.

In the section cited by the Examiner, the Dacier reference discloses (emphasis added below):

> "A set of signalling and routing protocols called Private Network-to-Network Interface (PNNI) standards is used on Asynchronous Transfer Mode (ATM) networks. PNNI is a comprehensive signalling standard providing dynamic routing capabilities and supporting Quality of Service (QoS) parameters for ATM networks. PNNI standards have been approved by the ATM Forum in 1996 and are described in a March 1966 publication by the ATM Forum called"Private Network to Network Interface Specification Version 1.0". This publication is hereby incorporated by reference.
>
> In order to establish and update routing paths and to reroute a path in case of link failure ATM network switches have to know the network's topology. It is necessary for a switch to know whether there is an available network path through it that has the required bandwidth and can support end-to-end QoS before that switch can accept a call without compromising the call's integrity. To this end, each switch maintains a database of the networks topology. To reduce the amount of information each switch has to maintain in its database about the topology of the network, the PNNI standard provides that the network can be logically defined as a hierarchy with nodes on each level of the hierarchy arranged in peer groups.
>
> Under PNNI, the switches exchange information with one another on a regular basis to inform every switch about changes in the topology of the network. The information exchange is performed using a process called"flooding". Flooding involves a hop-by-hop propagation of topology information in packets to all the switches in a peer group and to adjoining switches of other peer groups. Information about network topology is provided in PNNI Topology State Elements (PTSEs). When a PTSE is received at a switch, it is acknowledged by sending an acknowledgement packet back to the sending switch. If the PTSE contains information which is new or of more recent origin than that stored in the database of a receiving switch, that data is placed in the database for the receiving switch and the PTSE is transmitted to all neighbor switches of the receiving switch except the one from which the PTSE was received." (column 1, lines 14-52)

Thus, the Dacier reference discloses that switches in a peer group, as well as adjoining switches, exchange information in the form of a PTSE packet, and that when a PTSE packet is received by a switch, the receiving switch sends an acknowledgement packet to the switch that sent the PTSE packet.

However, this disclosure of the Dacier reference is not the same as the claimed "establishing a TCP connection, corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and the server only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet" (emphasis added). The Dacier reference does not teach or suggest that the acknowledgment packet, which the switch receiving the PTSE packet sends in response to the PTSE packet, is responded to by the switch which sends the PTSE packet. Thus, the switch which receives the PTSE packet, and sends the acknowledgement packet, is not expecting a response to the acknowledgement packet, and therefore there can be no conditional establishment of a connection depending upon the receipt of the response to the acknowledgement packet. Thus, the Dacier reference fails to teach or suggest establishing a TCP connection "only if the TCP proxy receives a response from the host to the SYN/ACK packet corresponding to the particular SYN packet" (emphasis added).

Therefore, the Poletto and Dacier references fail to teach or suggest the Applicant's claimed invention as a whole.

As such, Applicant submits that independent claim 7 is not obvious and fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

Therefore, Applicant respectfully requests that the rejection against claim 7 be withdrawn.

Claims 8 and 9

The Poletto and Darcier references alone or in combination fail to teach or suggest Applicant's invention as a whole, as recited in claim 8.

Specifically, the Poletto and Dacier references fail to teach or suggest at least "if packets in the sampling indicate an attack against the server, altering the

operation of the switch to forward all packets destined for the server to the processor" as recited in the claim as amended.

Poletto discloses "a system architecture for thwarting denial of service attacks on a victim data center" (abstract). However, as the Examiner acknowledges:

> "... [Poletto] does not explicitly teach if packets in said sampling indicate an attack against said server, altering the operation of said switch to forward all packets destined for said server to said processor." (page 3 of the 8/10/05 Office Action, emphasis added)

The Darcier reference fails to bridge the substantial gap between the Poletto reference and Applicant's invention as recited in claim 8. The Dacier reference discloses a switch in an ATM network which operates in a learning mode and an active mode. Regarding the Dacier reference, the Examiner alleges:

> "In the same field of endeavor, Dacier teaches a system and method for detecting attacks where upon detection all packets are forwarded (Dacier, col. 5, line 4 - col. 6, line 6)." (page 3 of the 8/10/05 Office Action, emphasis added)

Thus, the Examiner alleges that the Dacier reference discloses forwarding all packets upon detecting an attack. However, the Applicants respectfully disagree.

In the section cited by the Examiner, the Dacier reference discloses (emphasis added below):

> "Referring now to FIG. 4, in the PNNI protocol, a checking switch checks for receipt of a new reachability 40. On the receipt of a PTSE if a new reachability is received, we proceed to the process of the invention. The process of the invention then determines from the model if the checking switch is in learning mode or active mode 42. In learning mode, the switch first clears its database of all reachability data. Then as each new reachability is added to the database, the system checks for further new reachabilities. This continues until the end of the learning mode phase. At the end of the learning mode phase, the database of the checking switch contains all the reachability sets advertised by each node during the learning mode phase in accordance with the PNNI protocol.
>
> Upon the receipt of a PTSE while the network is operating in the active mode phase, the checking switch examines the reachability to determine if it is new 44. If it is new, it adds the

reachability 43 and if the new reachability overlaps any of the reachabilities of the switches in the peer group, the number of bits in the prefix of the new reachability are counted 46 and compared with the number of hits (or length) of the overlapped reachabilities. If the prefix of the new reachability is sufficiently longer (say four bits) than the prefix of any overlapped reachability, the overlapping is ignored and the check of the new reachability ends. However, if the prefix of the new reachability is less than the specified limit (here 4 bits) then the logic determines that the new reachability is suspicious. After it has been determined that the reachability is suspicious, an alarm is triggered 47 and the network supervisor is notified to determine if the new reachability is problematic 48. If the supervisor determines that the reachability does not constitute a problem, the check of the new reachability ends. If the new reachability is problematic, the problem is corrected 49 by the supervisor.

Of course, it is desirable to limit the number of false alarms that are triggered. This can be done by raising the number of bits by which the prefix of the new reachability must exceed any overlapped reachability before the overlapping is considered nonsuspicious. This is done at the risk of missing a problematic reachability. An alternative would be to examine the significance of the switches in the peer group 43, and establish individual levels that must be exceeded that depend on the criticality of the switch. Also, the program can look at the number of alarms that occur in a fixed period of time, and if there are multiple sources for the overwriting reachabilities in order to limit the number of alarms that are set.

Referring now to FIG. 5, each node contains a processor 50 which has associated through a bus 52 with program memory elements or computer usable media 54 containing software that performs the functions of FIG. 4. It also has data memory elements 56 which the reachabilities and identities of the other switches of the peer group are retained, working memory elements 58 which is used in performing the steps outlined in FIG. 4 and a input/output interface 59 for the receipt and transfer of the PTSEs on the network.

As shown in FIG. 6, upon receipt of a PTSE packet by the switch before the PNNI flooding protocol 62 is initiated. The reachability advertised by the sending node is checked by the intrusion detection algorithm 64 to see if the packet is suspicious as established by the requirements of the algorithm illustrated in FIG. 4. If the algorithm is violated, an alarm is set off for the supervisor to determine if the reachability is problematic and to institute the appropriate remedy including removing the problematic reachability

> from any other switch, and possibly removing the sending switch from the network."

Thus, the Dacier reference discloses, in response to the determination of a suspicious reachability, notifying a supervisor. The supervisor then corrects the problem, which can include removing the suspicious reachability from other switches and removing the switch which sent the suspicious reachability from the network.

However, this disclosure of the Dacier reference is not the same as the claimed "if packets in the sampling indicate an attack against the server, altering the operation of the switch to forward all packets destined for the server to the processor". Dacier does not teach or suggest forwarding any packets, let alone all packets, upon the determination of a suspicious reachability. As discussed above, the Dacier reference only discloses notifying a supervisor, removing the reachability from other switches, and removing the sending switch from the network.

Thus, the Poletto and Dacier references fail to teach or suggest the Applicant's claimed invention as a whole.

As such, Applicant submits that independent claim 8 is not obvious and fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder. Furthermore, claim 9 depends directly from independent claim 8 and recites additional limitations thereof. As such, and for at least the same reasons discussed above, Applicant submits that this dependent claims also fully satisfies the requirements under 35 U.S.C. §103 and is patentable thereunder.

Therefore, Applicant respectfully requests that the rejection be withdrawn.

CONCLUSION

Thus, Applicant submits that claims 7-9 are in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application,

it is requested that the Examiner telephone Eamon J. Wall at (732) 383-1438 or Stephen Guzzi at (732) 383-1405 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

10/27/05

E Wall

Eamon J. Wall, Attorney
Reg. No. 39,414
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Suite 100
Shrewsbury, New Jersey 07702